Cybersecurity in the Space Age

*Michael Potter**

Abstract

Legal aspects of cybersecurity in the space age are issues that both includes and transcends issues of outer space assets, space activities and outer space law. In the case of cybersecurity the spectrum includes space law, international law and domestic law. Without a clear understanding of the importance of cybersecurity in the space age, and without the most basic definitions of cyberattacks and WMDs there remains an increased level of instability, legal confusion, a lack of deterrence, and chaos in the international system. Due to the international intervention into Iraq over the past decades, the term Weapons of Mass Destruction (WMDs) has often been viewed as an over-politicized term. And more importantly many are inclined to believe that accusations of WMDs were cynically and disingenuously used by aggressor nations to manipulate the international system and as a pretext for war in the case of Iraq. And while there is virtually no consensus dealing with cyberattacks in the international system, there is certainly no consensus on the role and legality of digital and physical counter-attacks to combat cyberattacks both generally, as well as those of a potential WMD magnitude.

It would be understandable then, that politically and legally it may not be seen, as a convenient or an appropriate moment in history, to call for a reassessment and a thoughtful clarification of the definition and more importantly to ensure that a clarified definition of WMDs enables certain types and classifications of cyberattacks to be considered as WMDs.

* International Institute of Space Commerce, USA. 21 years ago in Jerusalem at the IAC, this author presented a paper entitled "The Outer Space-Cyberspace Nexus: Satellite Crimes." The paper suggested a framework for analytically understanding the outer space-cyberspace nexus, which I believe is still of relevance. More recently there have been arguments that "cyberspace" is dead. Decades ago we had to fight to enter a portal and immerse ourselves into cyberspace. In the internet of things, we are now immersed. In fact we have to fight, if we want to extricate ourselves from cyberspace. The argument suggest that cyberspace is so ubiquitous, that it is essentially meaningless. Today I would argue that there is not just a nexus, but a collision of cyberspace and outer space. I believe the more interesting question is whether the news of the death of cyberspace is premature?

I. Introduction

By the time you finish this sentence, computer hackers from around the globe will have made at least 1,000 attempts to breach the Pentagon's firewall.[1] If this has not captured your attention, consider that tens of billions of dollars will be allocated in the next 5 years for both cybersecurity and the security of space assets.[2]

On a daily basis cybersecurity becomes more urgent and more visible. In current events the difficulties that Secretary of State Hillary Clinton has confronted as a result of moving sensitive government email traffic to her personal server has attracted almost a global fascination. In fact it was alleged that some of her emails contained sensitive satellite photos of North Korean nuclear capabilities.[3] Even the most recent Tom Cruise movie, "Mission Impossible: Rogue Nation," starts off with a scene of special agents hacking a Russian satellite. Cyberattacks are growing exponentially. This urgency was highlighted earlier in the year when the White House held a cybersecurity summit in Palo Alto, California.[4] This paper is not intended as a final and definitive work on the subject of cybersecurity and of cyberattacks within international and space law. The paper is written in the spirit of initiating a discussion and a debate on the future of these issues and as a motivation to policymakers and to the international legal community to begin to take sensible and effective actions.

In a post Cold War era, in a time of multipolarity, while nuclear weapons remain very important, their day-to-day strategic significance can be said to have diminished as the threats of both terrorism and cyberattacks accelerate in the direction toward Weapons of Mass Destruction (WMDs). In this paper the author argues the term "cybersecurity" remains a relevant and useful term, and a helpful way to organize our thoughts, our defenses and our responses to Internet, cyber and satellite related security.

How important is the cybersecurity in the space age? Consider that during the height of the Cold War, one of the few justifications for all out nuclear

1 "On the Frontlines of Cyber War," By Damon Cline, Augusta Magazine, April 2015. www.augustamagazine.com/Augusta-Magazine/April-2015-1/On-the-Frontlines-of-Cyber-War/.

2 "US Commits $5B In NEW $$ To Countering Space Threats; HASC Protects It," By Colin Clark, April 22, 2014. http://breakingdefense.com/2015/04/us-commits-5b-in-new-to-countering-space-threats-china-russia/.

3 Clinton emails contained spy satellite data on North Korean nukes Revelation among biggest concerns inside intel community, By John Solomon, The Washington Times, September 1, 2015.

4 The New Cold War Is Going Digital And that's a problem, because deterrence doesn't work when it comes to cyberattacks, Heather Roff, August 13, 2013, Slate.Com. www.slate.com/articles/technology/future_tense/2015/08/russia_joint_chiefs_of_staff_hack_deterrence_doesn_t_work_with_cyberattacks.html.

war, would have resulted from an adversary conducting a preemptive attack on defense early warning reconnaissance satellites. The entire premise of the nuclear strategic concept of Mutually Assured Destruction (MAD) necessitates reliance on timely and accurate assessment of whether the enemy had launched nuclear equipped missiles. With early warning satellites, outer space was militarized, but not weaponized. Today an attack on early warning space reconnaissance satellites might be able to be achieved, most efficiently through a cyberattack rather than a traditional physical military attack.

To place cybersecurity into a powerful context consider that for nearly 20 years the U.S. nuclear launch code at all the minuteman silos was eight 0s.[5] And even now, a former U.S. commander is arguing that we should take nuclear missiles off of high alert, to minimize the possibility of a cyberattack.[6]

A Pentagon-sponsored report warns that the United States faces new threats from mass destruction weapons in the form of cyber, electronic and financial attacks, in addition to more well-known dangers from nuclear, chemical and biological WMDs.

> "In addition to the prolific conventional [weapons of mass destruction] threats posed by a vast network of state and non-state actors, the U.S. must also contend with emerging threats that are not conventionally recognized as WMD [...]
> Very few of America's adversaries will attempt to challenge the unmatched strength of the U.S. military in a traditional conflict, but they may employ alternative asymmetric approaches ... it is therefore necessary to consider emergent, nontraditional threats, such as cyber, electromagnetic pulse (EMP), and economic attacks, in a comprehensive discussion of WMD threats."[7]

Vice Admiral Arthur Cebrowski, recently asserted that:

> "Although a cyber-attack is digital, not physical, it is a threat that could physically harm thousands or tens of thousands of people. *It's likely that we will confront more cyber-attacks than chemical or dirty bomb attacks given the ease of which rogue states and non-state malicious parties can engage and given the difficulty of deterrence.* Physical harm is physical harm, regardless of the attack vec-

5 "FOR NEARLY TWO DECADES THE NUCLEAR LAUNCH CODE AT ALL MINUTEMAN SILOS IN THE UNITED STATES WAS 00000000" Today I Found Out, Karl Smallwood, November 29, 2013. www.todayifoundout.com/index.php/2013/11/nearly-two-decades-nuclear-launch-code-minuteman-silos-united-states-00000000/.

6 "Former U.S. commander: Take nuclear missiles off high alert," Robert Burns, April 30, 2015. www.airforcetimes.com/story/military/2015/04/29/former-us-commander-take-nuclear-missiles-off-high-alert/26603763/.

7 "Inside the Ring: New WMD threats," Bill Gertz, The Washington Times, www.washingtontimes.com/news/2012/oct/10/inside-the-ring-new-wmd-threats/?page=all.

> tor. We must therefore think of WMD in results-centric terms, not device-centric terms."[8]

I would like to provide an example of a significant current event, not in an effort to politicize this discussion, but in an effort to more broadly inform this discussion. It is instructive to look at the recent case of the lifting of the embargo on Iran, as part of an international effort to slow the Iranian development of nuclear weapons. This international agreement permits $ 100 billion of frozen Iranian funds to go to Tehran. It is well know that Iran has a vigorous cyberattack capability, even including a dedicated group of government sanctioned hackers with, the rather curious name of, "Rocket Kitten."[9] Even if Iran possessed a nuclear bomb today, it is not clear if this particular Weapon of Mass Destruction would confer a tremendous amount of immediate, leveragable, tactical advantage. However it is very clear that tens of billions of unfrozen dollars could be allocated by the Iranian regime for the support of conventional conflicts, terrorism and in particular, the subject of this paper, cyberattacks could be quite significant tactical and strategic value for Iran. In fact Ian Bremmer recently argued that Tehran successfully reverse-engineered the powerful Stuxnet worm created by the NSA and Israel before turning "it into their own cyber-weapons [...]".[10]
As a non-traditional threat, cyber warfare is highly leveragable. The cost of entry into the cyberwarfare area is extremely minimal, with satellite access, broadband access and remote low-cost leasable supercomputer capabilities. According to David Stupples the: "Iranians "have now realized they have a much stronger weapon at hand," he said. "If they pour resources into that,

---

8 "Results- vs. Device-Centric Threats: Why Cyber-Attacks Should be in the WMD Conversation," https://blogs.mcafee.com/executive-perspectives/results-vs-device-centric-threats-cyber-attacks-wmd-conversation/. Also See: Vice Admiral Arthur Cebrowski, Proceedings 1998, PIRACY 2.0: THE NET-CENTRIC EVOLUTION, http://cimsec.org/piracy-2-0-net-centric-evolution/18343.

9 "Iran-Linked Espionage Group Continues Attacks on Middle East," Security Week, Eduard Kovacs, September 2, 2015, www.securityweek.com/iran-linked-espionage-group-continues-attacks-middle-east.

10 "[...] to destroy Saudi Aramco's servers and nearly stop the kingdom's oil production [...] The US is losing its cyber edge and 'a black swan event' is increasingly likely The cyber gap between the US and its adversaries is only expected to narrow as nation-states and hacktivists invest more time and money learning how to spy on, steal from, and destroy digital systems." BREMMER: The US is losing its cyber edge and 'a black swan event' is increasingly likely,' Natasha Bertrand, May 8, 2015, Business Insider. www.businessinsider.com/bremmer-and-cyberwarfare-2015-5 Also look at: EXCLUSIVE: U.S. officials conclude Iran deal violates federal lawwww.foxnews .com/politics/2015/10/09/exclusive-us-officials-conclude-iran-deal-violates-federal-law/.

they can continually attack and continually get payoffs from their activities, quite cheaply."[11]

From a military perspective, bandwidth and frequency are now almost more important than bombs and boots. Countries whom organize for conventional warfighting capabilities, now find themselves involved with a new arms race for control of bandwidth inside the battlefield. Army's have gone high-tech and have now implemented user-friendly visualizations of the spectrum's real-time status on the battlefield. Soldiers can now pinpoint which locations are securely in electromagnetic control and which are susceptible to electronic attack. Leaders will soon "discover that no amount of firepower can assure its dominance."[12]

Some analysts are arguing that nationstate hackers maintain a weapon of mass destruction that is significant threat to the U.S. infrastructure. According to "a Department of Homeland Security official, network inspections had "found software tools left behind that could be used to destroy infrastructure components," following hacks from Russia and China. "It's like (improvised explosive devices) in Iraq. Bomb makers have certain signatures, and looking at a bomb, you can tell who and where that signature comes from."[13]

II. Weapons of Mass Destruction (WMDs) Definitional Issues

In fact what makes the subject of cyberattacks in the international system bedeviling is that it quickly morphs into the similar discussion of how international law and international organizations ought to deal with war in the international system. Over the last many decades war has proven to be difficult for the international system to effectively legislate, regulate, control or halt. Sadly the control of cyberattacks in the international system are likely also to remain elusive in the decades ahead.

Nevertheless definitions are important. Cyberattacks originate across a spectrum, from sole actors, to state actors and syndicates and groups that are driven by ideology or profit motive. As cybersecurity relates to satellite cybersecurity the emphasis should primarily be on the state actors, and non-traditional state-like actors and proxies rather than the lone unattached, unaffiliated hackers. Cyberattacks are a continuation of politics and the continuation of war by electronic and cyber means. To riff-off a well known aphorism, "power grows out of a hacked network."

---

11 "Cyber War Rages Between Iran, US," Voice of America, March 3, 2014. Al Pessin, www.voanews.com/content/cyber-war-rages-between-iran-united-states/2666299.html.

12 Inside the New Arms Race to Control Bandwidth on the Battlefield, www.wired.com/2014/02/spectrum-warfare/.

13 Chinese Hackers Have A Weapon Of Mass Destruction That No One Is Talking About, Business Insider, Geoffrey Ingersoll Feb. 22, 2013, www.businessinsider.com /mandiant-china-hackers-wmd-no-one-mentions-2013-2#ixzz3YJhbYVTM.

What makes cyberattacks difficult under international law and the "law" of popular opinion is that conflict and war are generally focused on violence and physical and "kinetic" operations. In a recent article entitled, "Cyber Operations and the Jus in Bello: Key Issues," Michael Schmitt argues, "Cyber operations can unquestionably generate such [physical] consequences even though they launch no physical force themselves. For instance, a cyber operation against an air traffic control system would place aircraft, whether military or civilian, at risk. Or one targeting a dam could result in the release of waters, thereby endangering persons and property downstream. In neither case would the actual act be destructive, but in both the consequences would be. Referring back to the requirement of violence, and its development in Additional Protocol I, cyber operations can therefore qualify as "attacks," even though they are not themselves "violent," because they have "violent consequences." A cyber operation, like any other operation, is an attack when resulting in death or injury of individuals, whether civilians or combatants, or damage to or destruction of objects, whether military objectives or civilian objects."[14] It is worth noting, that "The annual, global economic cost of cyber-attacks have now reached more than $ 400 billion, with about a quarter of that coming from just the U.S.[15]

In the context of Iran, it is probably not widely understood, that the country's current development of Intercontinental Ballistic Missiles (ICBMs). ICBMs falls into a troublesome definitional category. ICBMs are considered to be a WMD, according to the U.S. Department of Defense.[16] The significance of the words "separable" and "divisible" part of the weapon is that missiles such as SCUDs are considered weapons of mass destruction, while aircraft capable of carrying bombs are currently not. It is interesting to note that, the Proliferation Security Initiative (PSI) a global effort that aims to stop trafficking of weapons of mass destruction (WMD), their delivery systems, and

14 "Cyber Operations and the Jus in Bello: Key Issues," Michael Schmitt, http://law.huji.ac.il/upload/6_Housen-Couriel.pdf.

15 "See What Elon Musk's Right Hand Man Has to Say About Cyber Hackers," Andrea Tse, www.thestreet.com/story/12441320/1/See-what-elon-musks-right-hand-man-has-to-say-about-cyber-hackers.html.

16 "weapons of mass destruction" (DOD) Chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties, and excluding the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon. Also called WMD. See also special operations. Source: JP 3-40," See DoD Dictionary of Military Terms. See also In 2004, the United Kingdom's Butler Review recognized employed the definition of United Nations Security Council Resolution 687, which defined the systems which Iraq was required to abandon:Ballistic missiles with a range greater than 150 Ballistic missiles with a range greater than 150 kilometres and related major parts, and repair and production facilities.kilometres and related major parts, and repair and production facilities.

related materials, to and from states and non-state actors of proliferation concern, was originally created to stop the shipment of SCUD missiles.[17]
Separately, under U.S. federal law, the 9-11 attacks on the World Trace Center would be defined as a WMD, because under U.S. law a "destructive device," include any "explosive," any "bomb,"[18] and in addition the WTC attacks, the terrorists used the fuel of the airplane as their weapon. The airplanes contained 60 tons of fuel each. Aviation fuel contains 10x the energy, gram per gram, as TNT. The potential energy was equivalent to about 600 tons of TNT, more than half a kiloton.[19]
I believe that commonly accepted international law too narrowly defines WMDs, while U.S. domestic law defines WMDs far too broadly defined. However under U.S. law there are the concepts that it is illegal to "conspire" to attempt to create as well as it is illegal to use "any combination of parts" towards creating WMDs. These could be a useful concepts in international law. A threshold for considering cyberattacks a WMD might include cyberattacks targeting civilians, cyberattacks on civilian aviation, cyberattacks on community water systems and energy systems, attacks on railroads, highway signaling systems, space systems, and even on a nation's commercial and financial systems. The distinguishing elements, are civilians, scale, proportionality, and financial impact. Routine low level information probes and data gathering as an international practice seems to have become generally accepted.
Current international law does not provide sufficient language in which the law is able to properly view cyberattacks in the framework of WMD. I would argue similarly, that in the case of cybersecurity when a significant portion of a network is dedicated to delivering a cyberattack of WMD magnitude, that "network" portion of the dedicated network, ought to be classified as a WMD. Of importance the network could be construed, as a legitimate target in the international system. In a recent paper, on the disruption of satellite transmission it was argued,

> "The as-yet unresolved issue of whether a virtual attack on a satellite system is in fact an armed attack under the Charter is a compelling one to an increasing number of states: more and more, state and non-state actors are interested in knowing under what circumstances disruption of a satellite transmission consti-

17 "The Proliferation Security Initiative: Can Interdiction Stop Proliferation?" Jofi Joseph, www.armscontrol.org/print/1579.
18 18 U.S. Code §2332a – Use of weapons of mass destruction | US Law | LII / Legal Information Institute, https://www.law.cornell.edu/uscode/text/18/2332a.
19 "Analysis of the Terrorist Attack,". Department of Physics at the University of California at Berkeley, and Faculty Senior Scientist at the Lawrence Berkeley Laboratory, where I am also associated with the Institute for Nuclear and Particle Astrophysics. http://muller.lbl.gov/pages/Analysis_of_the_attack.htm.

> tutes an attack act that justifies self-defense; and what the parameters of legitimate response to such an act may be."[20]

But there is a substantial change in the nature of the activity when it turns to destruction of property and the infliction of harm on civilians. When that threshold is crossed the country that has become victim to such an attack, could arguably have a legitimate basis to launch a physical attack on the country and the cyber infrastructure of the perpetrators. A nation inflicting offensive destruction, perhaps, may be seen as losing what is normally viewed as an acceptable capability to monitor and probe. This would be a significant departure from the norms of the Cold War.

III. Space & Cold – Strategic Threat[21]

III.1. A Framework of Threats

In a recent presentation titled "Satellite hacking," a popular IT security expert listed the following top 10 threats:[22]

III.2. A Brief Current Overview of Satellite & Strategic Issues

In a recent CBS television news piece on U.S. satellite vulnerability, "A White House document obtained by 60 Minutes estimates the Pentagon spends about $ 25 billion a year on space – more than NASA or any other space agency in the world. The estimate includes spy satellites and other classified spending. In a statement, the Chinese embassy in Washington, DC, told 60 Minutes that China is "committed to the peaceful use of outer space." [...]

---

20 "DISRUPTION OF SATELLITE TRANSMISSIONS UNDER IHL: LAUNCHING NEW PARADIGMS," Deborah Housen-Couriel, http://law.huji.ac.il/upload/6_Housen-Couriel.pdf.

21 In the late nineteen-fifties, "US intelligence developed what seemed like a useful technology: equipment that could tamper with the electronics of orbiting satellites; theoretically, such a device could even be used to take control of an orbiting object. The equipment was tested, but just before somebody pointed it at a Soviet satellite, intelligence officers contacted a consultant with the National Security Agency to hear his thoughts. He shot the plan down quickly, said the idea was a very, very bad one. By using the equipment, he argued, America would be setting the precedent that it was acceptable for countries to tamper with each other's satellites, and if everyone started doing it, nobody would be able to use satellites at all. The equipment was disabled to ensure that no one would ever use it, even by accident." "The Dirty Secrets Behind the Race to Put a Man on the Moon," Kurt Eichenwald, NewsWeek, September 17, 2014. www.newsweek.com/2014/09/26/dirty-secrets-behind-race-put-man-moon-271158.html.

22 Hacking Satellites … Look Up to the Sky – InfoSec Resources, September 18, 2013. http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/ Also See: WTA Urges Teleport Operators to Improve on Cybersecurity, By Juliet van Wagenen, August 5, 2015. www.satellitetoday.com/technology/2015/08/05/wta-urges-teleport-operators-to-improve-on-cyber-security/.

Gen. Hyten says the U.S. wants peace but must be prepared for conflict. "It's a competition that I wish wasn't occurring, but it is," says Hyten. "If we're threatened in space [...] we have the right of self-defense [...] and we'll make sure we can execute that right."[23]

The top cyber official for the Air Force says the service's space and satellite networks are being constantly hacked by outside groups. "There's millions of probes every year into our networks, from every corner of the world," according Gen. John Hyten, the head of Air Force Space Command, "Those probes come from everything, from nation states down to individuals just curious, down to criminal behavior," he added.[24]

For the U.S. the ground war in the Middle East, has now largely become an unregulated cyber-satellite war. While there may not be a lot of American "combat boots" in Syria, "dozens of manned and unmanned aircraft dot the skies above gathering video and other types of intelligence about the movement of Islamic State militants. The images collected by those aircraft are streamed by satellites in near real-time thousands of miles away to Langley Air Force Base in southern Virginia."[25]

Experts argue: "Iran is improving its cyber capabilities faster than experts 'would have ever imagined' and increased cyber-security spending 12-fold since 2013. Iran is training a new generation of cyber soldiers, According to a report released in 2013 by the Middle East Media Research Institute, by November 2010, the Basij Cyber Council had trained 1,500 cyber-warriors who, according to IRGC commander Hossein Hamedani, "have assumed their duties and will in the future carry out many operations."[26] "Although Chinese defense academics often publish on counterspace threat technologies, no additional anti satellite programs have been publicly acknowledged. PLA writings emphasize the necessity of "destroying, damaging, and interfering with the enemy's reconnaissance [...] and communications satellites," suggesting that such systems, as well as navigation and early warning satellites, could be among the targets of attacks designed to "blind and deafen the enemy." PLA analysis of U.S. and coalition military operations also states that "destroying or capturing satellites and other sensors [...] will deprive an opponent of ini-

---

23 "Critical U.S. satellites vulnerable?" – CBS News, April 24, 2015. www.cbsnews.com /news/preview-the-battle-above/?utm_content=buffer05833&utm_medium=social &utm_source=facebook.com&utm_campaign=buffer.

24 Cyber general: US satellite networks hit by 'millions' of hacks, http://thehill.com /policy/defense/240286-general-us-space-networks-probed-millions-of-times-annually.

25 A Look Inside a Secret US Air Force Intelligence Center – Defense One, www.defenseone.com/technology/2014/11/look-inside-secret-us-air-force-intelligence-center/99347/.

26 "Iran increased cyber-security spending 12-fold since 2013," March 28, 2015 By Pierluigi Paganini, http://securityaffairs.co/wordpress/35419/hacking/iran-cyber-capabilities.html.

tiative on the battlefield and [make it difficult] for them to bring their precision guided weapons into full play."[27]
In April 2015 the Pentagon released a Cybersecurity Strategy, which is a follow on to the original first-ever cyber strategy in 2011.

> "[...] with a warning to potential adversaries: The United States will no longer only be reactive in its cyber defenses, as the Pentagon will be armed and ready to retaliate against cyberattacks or even strike first to pre-empt them. The strategy is careful to note, however, that the U.S. seeks to exhaust all network defense and law enforcement options before moving to cyber operations."[28]

The U.S. Air Force, recently admitted the need to move toward a common satellite control system. The head of the U.S. Air Force Space Command General John Hyten argued, "that developing a separate ground system for each separate satellite program was the "dumbest thing in the world" and change was overdue." "[...] he told a news conference that "way too much money" had been spent on separate telemetry, tracking and control systems in recent years. "We're going to figure out how to spend that money once and have industry do the unique things that are unique to their satellite." Developing a common ground system would also help shore up the security of the networks used to communicate with, track and control the satellites, and it would make it far easier to train Air Force personnel, Hyten argued.[29] "For us, the balance in the future's going to be operating in those three domains of air, space and cyber," he said. "How do you manage the balance? Can you become more efficient or control costs while maintaining the same operational capability? If so – it's like nirvana."[30, 31, 32, 33]

---

27 Chinese Strategy and Military Power in 2014: Chinese, Japanese, Korean, Taiwanese and US Assessments Anthony H. Cordesman November 25, 2014 Rowman & Littlefield, https://play.google.com/store/books/details?id=nwfmBQAAQBAJ&rdid=book-nwfmBQAAQBAJ&rdot=1&source=gbs_vpt_read&pcampaignid=books_booksearch_viewport.

28 "Armed and Ready: The Pentagon's Assertive New Cyber Strategy," Eric Sterner, April 30, 2015. www.worldpoliticsreview.com/articles/15656/armed-and-ready-the-pentagon-s-assertive-new-cyber-strategy.

29 U.S. Air Force moves toward common satellite control system, Reuters, April 16, 2015. www.reuters.com/article/2015/04/16/us-usa-military-space-ground-idUSKBN0N72QO20150416.

30 The Pentagon's new cyber attack plan: 'Blunt force trauma,' By Philip Ewing, 04/18/15, www.politico.com/story/2015/04/dod-hopes-cyber-can-create-blunt-force-trauma-117095.html.

31 "NRO's Sapp Prods Unnamed Colleague on Resiliency," SpaceNews, Mike Gruss, June 30, 2015. http://spacenews.com/nros-sapp-prods-unnamed-colleague-on-resiliency/?utm_content=buffer18a94&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer.

The National Aeronautics and Space Administration was under heavy attack over the past two years, as adversaries tried to infect machines with malware or use advanced persistent threats to get into the network, according to Congressional testimony.
Attackers from a Chinese-based IP address had breached the network at NASA's Jet Propulsion Laboratory and gained full access to the networks and sensitive user accounts, NASA Inspector General Paul Martin told the House Science, Space and Technology committee, NASA made the discovery in November, and the JPL incident is still under investigation, according to Martin."[34]
In the past the International Space Station was hit by 'malware spread from infected devices in orbit: "Russian cosmonauts managed to carry infected USB storage devices aboard the station spreading computer viruses to the connected computers. The damage done by the malware to the computer systems of the ISS is unknown. However, Kaspersky said virus epidemics took hold of the space-based computers, including dozens of laptops. "It's not a frequent occurrence, but this isn't the first time," a NASA spokesperson said at the time. In May, the United Space Alliance, which oversees the running of if the ISS in orbit, migrated all the computer systems related to the ISS over to Linux for security, stability and reliability reasons."[35]
One of the most popular cases of satellite eavesdropping has as a protagonist the off-shelf software SkyGrabber, produced by the Russian firm Sky Software and sold for $ 26. The software can be used by hackers in Iraq and Afghanistan to capture unencrypted video feeds of the Predator unmanned aerial vehicles (UAVs).[36]
The best known of alleged takeovers of satellite control occurred in 2007 and 2008. In particular, a serious attack was observed in 2008 when hackers obtained the control of the NASA Terra EOS earth observation system satellite for 2 minutes in June and for another 9 minutes in October. Fortunately the attackers didn't damage the satellite during the time they gained control of it. The incident took place in July of 2008. Unlike the Terra EOS incident, this

---

32 "Air Force charges new cyber task force with looking for threats in core missions," JARED SERBU, APRIL 18, 2015, http://federalnewsradio.com/defense/2015/04/air-force-charges-new-cyber-task-force-with-looking-for-threats-in-core-missions/.

33 "Space Combat Capability [...] Do We Have It?" Capt Adam P. Jodice, USAF Lt Col Mark R. Guerber, USAF, Air & Space Power Journal, Sept-Oct, 2015. www.airpower.maxwell.af.mil/article.asp?id=238.

34 NASA Has Been Under Heavy Cyber Attack – NASA Watch, By Marc Boucher on March 5, 2013 (A belated story about an earlier cyber attack). http://nasawatch.com/archives/2013/03/nasa-has-been-u.html.

35 International Space Station attacked by 'virus epidemics', The Guardian, November 12, 2013. www.theguardian.com/technology/2013/nov/12/international-space-station-virus-epidemics-malware.

36 Hacking Satellites … Look Up to the Sky – InfoSec Resources, September 18, 2013. http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/.

hack did gain access, but did not allow control to be gained.[37] Hackers from China breached the federal weather network recently, forcing cybersecurity teams to seal off data vital to disaster planning, aviation, shipping and scores of other crucial uses, officials said. The October satellite data outage meant that the National Weather Service and centers around the world did not receive large amounts of information. "A July report on NOAA by the Inspector General for the Commerce Department – where NOAA sits – criticized an array of "high-risk vulnerabilities" in the security of NOAA's satellite information and weather service systems. The report echoed the views of a 2009 audit from the IG that said the primary system that processes satellite data from two environmental and meteorological systems had "significant" security weaknesses, and that "a security breach could have severe or catastrophic adverse effects."[38] The incidents and examples above are remarkably compelling. But one aspect that touches the immediate lives of so many civilians and commercial air travel.

III.3. Hacking the Friendly Skies: A Framework for Aviation Cybersecurity

Currently, there is no common vision, or common strategy, goals, standards, implementation models, or international policies defining cybersecurity for commercial aviation. Globally aviation administration has fallen short in its efforts to protect the national air traffic control system from terrorists or others who might try to hack into the computers used to direct planes in flight, according to a government report. The Government Accountability Office report credited the Federal Aviation Administration with taking steps to deter hackers but concluded that "significant security control weaknesses remain, threatening the agency's ability to ensure the safe and uninterrupted operation of the national airspace."[39] According to the FAA document the vulnerability exists because the plane's computer systems connect the passenger network with the flight-safety, control and navigation network. It also connects to the airline's business and administrative-support network, which communicates maintenance issues to ground crews.

There was very publicised incident recently where a hacker, Chris Roberts was arrested for sniffing air-control data traffic and connecting his laptop to

37 "Hacking Satellites … Look Up to the Sky" – InfoSec Resources, September 18, 2013. http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/.

38 Chinese hack U.S. weather systems, satellite network, Mary Pat Flaherty, Jason Samenow and Lisa Rein November 12, 2014, www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html?utm_content=buffer980c3&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer.

39 FAA computers vulnerable to hackers, GAO report says. www.washingtonpost.com/local/trafficandcommuting/faa-computers-vulnerable-to-hackers-gao-report-says/2015/03/02/388219ac-c119-11e4-9271-610273846239_story.html.

the infotainment networks of a commercial passenger airplane."[40] Documents showed how inflight entertainment systems on some planes were connected to the passenger satellite phone network, which included functions for operating some cabin control systems. These systems were in turn connected to the plane avionics systems.

In a recent demonstration a U.S. government drone was hacked. According to news reports: "Spoofing a GPS receiver on a UAV is just another way of hijacking a plane," Humphreys told Fox. "In five or ten years you have 30,000 drones in the airspace, each one of these could be a potential missile used against us." "What if you could take down one of these drones delivering FedEx packages and use that as your missile?" Humphreys asks. "That's the same mentality the 9-11 attackers had."[41]

On the satellite portion of the network, Colby Moore, a researcher with the cybersecurity firm Synack, has found that it's relatively easy to crack Globalstar's GPS satellite network. This is a company that bills itself as "the world's most modern satellite network." GPS trackers beam data to satellites, which send them back to base stations on Earth. Using cheap hardware and small planes, Colby successfully intercepted and decoded data – none of which was encrypted.[42]

In addition satellite communications systems have security vulnerabilities that may allow hackers to gain access to aircraft systems, according to cyber security expert Ruben Santamarta, security consultant. Santamarta published a white paper that discusses security vulnerabilities in air, sea and land satcom systems, including systems made by Cobham and Iridium."[43]

Positioning, navigation and timing (PNT) has been at the foundation of military capability for centuries, required for functions ranging from navigating the seas to coordinating actions on the battlefield. Pseudolites, which provide an alternate signal that can be used to increase resilience for area protection.[44, 45] The Air Force has been in the process of modernizing GPS perfor-

---

40 "Feds Say That Banned Researcher Commandeered a Plane," Kim Setter, May 15, 2015, Wired Magazine, www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/.

41 U.S. Drone HACKED and HIJACKED With Ease! November 1, 2013. http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/.

42 GPS satellite networks are easy targets for hackers, Jose Pagliery, http://money.cnn.com/2015/08/04/technology/hack-space-satellites/.

43 "U.S. Drone HACKED and HIJACKED With Ease!" Matt Thurber – October 4, 2014, www.ainonline.com/aviation-news/2014-10-04/security-expert-raises-issues-satcom-vulnerabilities.

44 "Assured PNT: A path to resilient positioning, navigation and timing," http://peoiews.apg.army.mil/news_Assured_PNT.html?utm_content=buffer4f8a6&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer.

45 For example, on April 1, the Russian GNSS GLONASS suffered an unprecedented total disruption of its entire system where positioning was valueless for almost 11

mance and security.[46] The purpose of "Information Assurance" IA, also referred to as cyber security, is to ensure that DOD systems can resist and continue to operate during cyber-attacks by managing risks and implementing safeguards. Gen. John Hyten, the Air Force Space Command commander, recently stated: "The good thing about having space and cyberspace in one command is we can actually integrate the capabilities of space and cyber and figure out how we're putting those pieces together. That's what we're trying to do. All the networks are invisible, but everything is connected [...] everything has to work together."[47] An emerging doctrine in the U.S. military circles is the subject of cyber counter-attacks.

IV. Counter Attack

Cyber-security is tricky because it represents what former, Richard Clarke, former U.S. National Coordinator for Security, Infrastructure Protection, and Counter-terrorism calls an "offense preference."

> "It costs thousands of times more money to defend your resources from a digital attack than to perpetrate one. Many companies have sprung up with the goal of providing cyber-security to companies. Their wares, however, constitute little more than Band-Aid measures that can temporarily deter hacking before a work-around is developed."[48]

One recent analyst asked "if attacking the hackers was the next security frontier?"[49] Counter-attacks to deal with cyberattacks can be both of a physical and digital nature. Counter-attack have also been termed hacks back,"[50] and

---

hours. Reports that it was an error by a GLONASS engineer are challenged by others questioning if it was the result of a cyber attack or a powerful solar flare that erupted at about the same time.GPS jammers a top concern in maritime cyber readiness, Jun 3, 2014. www.professionalmariner.com/June-July-2014/GPS-jammers/.

46 "GPS Actions Needed to Address Ground System Development Problems and User Equipment Production Readiness," September 2015. www.gao.gov/assets/680/672367.pdf.

47 "AFSPC: Space, cyberspace provide advantages, challenges," By Tech. Sgt. Torri Hendrix, Secretary of the Air Force Public Affairs Command Information / Published September 16, 2015, www.af.mil/News/ArticleDisplay/tabid/223/Article/617413/afspc-space-cyberspace-provide-advantages-challenges.aspx.

48 "CMC talk addresses challenge of cyber-security and warfare," Sarah Torribio, February 20, 2015. https://www.claremont-courier.com/articles/news/t14454-cyber.

49 ATTACKING HACKERS: THE NEXT SECURITY FRONTIER? Payments, www.pymnts.com/in-depth/2015/attacking-hackers-the-next-security-frontier/#.VeEQjXi8HjI.

50 What Is Active Defense? (AKA Attack the Hackers), www.pymnts.com/in-depth/2015/attacking-hackers-the-next-security-frontier/#.VhBIl7SUDjI.

"active defense." These concepts of counter-attack inform the new U.S. cyber attack strategy Which calls for the ability to deliver 'blunt force trauma'.[51]

V. Conclusion

Although perhaps slightly overstated and sensationalist, analysts argue that we are engaged in and witnessing an active full-blown cyberwar and that hackers, at will, can now reach every satellite around the earth. Yet, it is true that cyberattacks are growing an exponential rate, which makes the issue of cyber attacks exponentially more relevant.

In the recent The Joint Comprehensive Plan of Action (JCPOA) agreement with Iran, neither WMDs of ICBMs and potential cyberattack WMDs have not been carefully considered, nor curtailed. There are many questions for international agreements such JCPOA. Who determines their legitimacy of the negotiators and of the agreement? Ironically in this case, Iran dictated exclusively who they considered to be "legitimate" negotiating parties for this agreement. More importantly if there are serious negative, or even deadly consequences that result from the failure of this regime, who should or would be held accountable, if anyone were ever to be held accountable at all? In negotiations such as JCPOA is it realistic and is it necessary to bring all the relevant parties to the negotiating table? If in the future, JCPOA is not considered to be a success, will critics dismiss these efforts as being the work of a small group of elite politicians, naive policymakers, and negotiators who intentionally created havoc in the international system?

It is instructive that during Chinese Premier Xi Jinping's recent visit to the United States, an unprecedented, yet rather modest baby step agreement for cyberspace between the two countries was signed. While the agreement represents a "first start, it also highlights long-standing shortfalls in U.S. preparedness and response capabilities in cyberspace beginning with a lack of well understood doctrine for cybersecurity." President Barack Obama "announced that he and Xi had agreed not to conduct or support cybertheft of business secrets. Obama called the agreement "a work in progress," while Xi agreed that the countries would abide by "norms of behavior" in cyberspace.[52]

This agreement is referred to as a "CERT agreement – that is, direct cooperation between Chinese and American law enforcement officials. If American commercial secrets are stolen, US law enforcement should now be able to call up their Chinese counterparts and expect real investigations and possibly

---

51 'Blunt force trauma' – Philip Ewing – POLITICO, www.politico.com/story/2015/04/dod-hopes-cyber-can-create-blunt-force-trauma-117095.

52 U.S.-China Cybersecurity Pact Highlights Bigger Issues – US News, By Daniel Gerstein, www.usnews.com/opinion/blogs/world-report/2015/09/26/us-china-cybersecurity-pact-highlights-bigger-issues.

even arrests as a result."[53] Joseph Steinberg assets that: "While some might argue that the US is better off with a bad deal or a partial deal than with no deal, and that any reduction of hacking is better than the present situation, or that the agreement is simply a framework for moving forward, I am not so sure. By announcing this agreement, the US government has granted some level of de-facto legitimization to activities that it should not be willing to tolerate."[54]
Daniel Gerstein argues,

> "Today, no such official doctrine guides international, or for that matter, U.S. cybersecurity policy. No comprehensive framework exists for thinking about cyberspace issues, managing concerns or even responding to crises. There are no set limitations on potentially destabilizing behavior. There's not even an internationally accepted glossary or terminology to guide creation of cyber norms."[55]

Cybersecurity in the space age is topic that both includes and transcends issues of outer space assets, space activities and outer space law. Without a clear understanding of the importance of cybersecurity in the space age, and without the most basic definitions of cyberattacks and WMDs there remains an increased level of instability and legal confusion and chaos in the international system. Without clear and accurate legal definitions there is also an important missing layer of deterrence in the international system. Nations will continue to mount vigorous cyberattacks against other nations. Most importantly these cyberattacks, when they exceed a certain magnitude and proportionality, and threaten civilians can be viewed as WMDs. The argument in favor of deterrence is to make sure that there is no sanctuary for those that seek to commit cyberattcks as a WMD. And while there is virtually no consensus dealing with cyberattacks in the international system, there is no consensus on the role and legality of digital and physical counter-attacks to combat cyberattacks of a potential WMD magnitude.
Internationally there are many overlaps and many holes in various international regimes. There are regimes that focus on nation states, on organized crime, on terrorism, on money laundering, radiological material, and on countless other transnational issues. Understandably, I am a bit reluctant to suggest yet another incomplete, and problematic regime. Nevertheless an

---

53 The new US-China cybersecurity agreement: a brief guideUpdated by Zack Beauchamp on September 25, 2015, www.vox.com/2015/9/25/9399117/obama-xi-cyber-economic.

54 "10 Issues With the China-US Cybersecurity Agreement," BY JOSEPH STEINBERG CEO, SecureMySocial, www.inc.com/joseph-steinberg/why-the-china-us-cybersecurity-agreement-will-fail.html.

55 U.S.-China Cybersecurity Pact Highlights Bigger Issues – US News, By Daniel Gerstein, www.usnews.com/opinion/blogs/world-report/2015/09/26/us-china-cybersecurity-pact-highlights-bigger-issues.

international framework of principles that could inspire a strategy for combating cyberattacks might be the Proliferation Security Initiative (PSI) a global effort that aims to stop trafficking of weapons of mass destruction (WMD), their delivery systems, and related materials.[56]

In the very near future it is conceivable that a nation will conduct a visible and powerful kinetic, military attack upon the physical cyber and network assets of a nation responsible for cyberattacks that approach the level of WMDs.

Very conceivably cyberattack WMDs will have some space and satellite nexus. The international legal community needs to collectively be prepared for this eventuality. If the international legal community fails to act, or fails to address these issues correctly, the community may in the future, be viewed, as almost providing a tacit acceptance of the development and non-regulations and enforcement of cyberattacks as a WMD. Nations will not wait for the international legal community to catch up with the exponential challenge of cyberattacks in the international system.

56 "Proliferation Security Initiative: Statement of Interdiction Principles," Fact Sheet, The White House, Office of the Press SecretaryWashington, DCSeptember 4, 2003. www.state.gov/t/isn/c27726.htm.